

**CLAIMS**

What is claimed is:

1. A method for handling cargo containers at transshipment points with a data management system, said method comprising;
  - 5 ensuring data input in a format acceptable to a system for identifying contents and tracking at least one particular container,
  - identifying each container by a profile,
  - checking said data input for each profile against a thesaurus-like data recognizer software program having access to multiple terms for at least one of
  - 10 the data inputs, and expanding the total amount of information kept for containers by matches in said thesaurus-like data recognizer software, thereby expanding said profile,
  - checking other sources against said profile and determining whether data in said expanded profile has reference of interest to other sources' trigger
  - 15 information, and if so, adding said reference of interest to further expand said profile,
  - checking business rules against the expanded total amount of information for said particular container to determine a security risk level for said further expanded profile,
  - 20 responding to said security risk level.
2. The method of claim 1 wherein said response to said security risk level is one of several responses including either
  - a) a manual search of said container,
  - 25 b) gamma irradiation inspection processing of said container and re-evaluation of said container's risk based on results of said irradiation inspection processing,
  - c) minimal inspection of container, and
  - d) allowing passage through checkpoint.

30

3. The method of claim 2 wherein said responses are chosen based on a scaled risk profile having a high risk side and a low risk side and wherein said step a is reserved for containers having been evaluated with a risk profile toward the high end of the scale.

5

4. The method of claim 3 wherein regardless of a risk profile's scale, said container is subject to response b, and if as a result of said response b, a higher risk profile is developed for said container, then applying response a to said container.

- 10 5. The method of claim 3 wherein a low risk profile garners a c and d response from the system.

6. The method of claim 5 wherein if in a c response, a suspicious circumstance is found, exercising response b.

15

7. The method of claim 5 wherein if in a c response, a suspicious circumstance is found, exercising response a.

- 20 8. The method of claim 5 wherein if in a c response, a suspicious circumstance is found, exercising response a.

9. The method of claim 2 wherein under circumstances where an operator has an option to increase the risk profile risk of any or all containers based upon external factors.

25

10. A system for handling cargo containers at transshipment points that recommends particular handling processes based upon a risk profile comprising:

a security module having access to

30

a thesaurus module,

a business rules module, and

a Knowledge Base module having means for accepting external data input,

wherein said security module is for receiving documentary data input for each said container, and for processing said data through said thesaurus

5 and said knowledge base module according to business rules in said business rules module, and through said processing according to said business rules for producing said recommendation.

10 11. The system of claim 10 wherein said recommendation corresponds to at least one of several handling processes.

12. The system of claim 11 wherein said handling processes comprises:

a) a manual search of said container,

15 b) gamma irradiation inspection processing of said container and re-evaluation of said container's risk based on results of said irradiation inspection processing,

c) minimal inspection of container, and

d) allowing passage through checkpoint.

20 13. The system of claim 12 wherein said security module has software for choosing responses based on a scaled risk profile having a high risk side and a low risk side and wherein said step a is reserved for containers having been evaluated with a risk profile toward the high end of the scale.

25 14. The system of claim 13 wherein regardless of a risk profile's scale, said security module software recommends that said container is subject to response b, and if as a result of said response b, a higher risk profile is developed for said container, then said security module software recommends applying response a to said container.

30

15. The system of claim 14 wherein if in a c response, a suspicious circumstance is found, said security module software recommends exercising response b.
- 5 16. The system of claim 5 wherein if in a c response, a suspicious circumstance is found, said security module software recommends exercising response a.
- 10 17. A port system for handling cargo containers at transshipment points that recommends and executes particular handling processes based upon a risk profile, and processes said cargo containers before releasing them through said transshipment point comprising:
- inspection facilities having a manual inspection crew, a gamma irradiation inspection processing facility, and a secure checkpoint, and
- a security module having access to
- 15 a thesaurus module,
- a business rules module, and
- a knowledge base module having means for accepting external data input,
- 20 wherein said security module is for receiving documentary data input for each said container, and for processing said data through said thesaurus and said knowledge base module according to business rules in said business rules module, and through said processing according to said business rules for producing said recommendation.
- 25 18. The system of claim 12 wherein said recommendation corresponds to at least one of several handling processes.
19. The system of claim 13 wherein said handling processes comprises:
- a) a manual search of said container,

b) gamma irradiation inspection processing of said container and re-evaluation of said container's risk based on results of said irradiation inspection processing,

c) minimal inspection of container, and

d) allowing passage through checkpoint.

5